(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 281 057 A2**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **88103012.6**

(51) Int. Cl.⁴: **G07F 7/10** , G07C 9/00

(22) Anmeldetag: **29.02.88**

(30) Priorität: **04.03.87 DE 3706955**
12.08.87 DE 3726881

(43) Veröffentlichungstag der Anmeldung:
07.09.88 Patentblatt 88/36

(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI LU NL SE

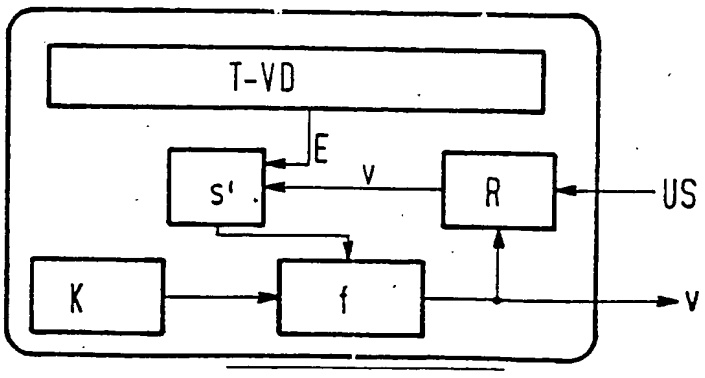
(71) Anmelder: **Siemens Aktiengesellschaft Berlin und München**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Beutelspacher, Albrecht, Prof.**
Schwalbenstrasse 78
D-8012 Ottobrunn(DE)
Erfinder: **Kersten, Annette-Gabriele**
Frauenlobstrasse 6
D-6200 Wiesbaden(DE)
Erfinder: **Kruse, Dietrich**
Ulmenstrasse 9
D-8012 Ottobrunn(DE)

(54) Schaltungsanordnung zur Sicherung des Zugangs zu einem Datenverarbeitungssystem mit Hilfe einer Chipkarte.

(57) Aus einem im Mikroprozessor der Chipkarte implementierten Chiffrieralgorithmus (f) und einem gespeicherten Geheimschlüssel (K) wird in Abhängigkeit von einem variablen Startwert (s) eine Zufallszahl gemäß der Beziehung v = f(K; s) generiert. Diese Zufallszahl kann in einem Register zwischengespeichert und bei der Generierung einer neuen Zufallszahl mit einer variablen Eingangsgröße, z.B. mit dem variablen Startwert (s) zu einem modifizierten variablen Startwert (s') logisch verknüpft werden.

FIG 5



EP 0 281 057 A2

Schaltungsanordnung zur Sicherung des Zugangs zu einem Datenverarbeitungssystem mit Hilfe einer Chipkarte

Die Erfindung betrifft eine Schaltungsanordnung nach den Merkmalen des Oberbegriffs des Anspruchs 1.

In modernen Datenverarbeitungs-und Kommunikationssystemen spielt der Schutz der Daten eine immer wichtigere Rolle. Die Qualität eines Systems in bezug auf einen ausreichenden Datenschutz hängt dabei entscheidend davon ab, inwieweit es gelingt, daß zur Zugriff zum System nur für berechtigte Personen möglich ist und umgekehrt nichtberechtigte Personen mit absoluter Sicherheit ausgesperrt bleiben. Eine einfache, wenn auch nicht absolut sichere Möglichkeit zur Überprüfung der Zugangsberechtigung zu einem System sind zum Beispiel sogenannte Paßwörter, die nur dem berechtigten Benutzer bekannt sind und die vom Benutzer beliebig oft geändert werden können. Da bei Paßwörtern die Gefahr besteht, daß sie von Unbefugten ausgespäht oder abgehört werden können, sind zusätzliche Sicherungsmaßnahmen unverzichtbar. Eine dieser Maßnahmen ist zum Beispiel die Ver-und Entschlüsselung der übertragenen Information, eine Maßnahme, die bei Datenverarbeitungssystemen unter anderem auch mit Hilfe der Chipkarte realisierbar ist.

Mit der zunehmenden Einbeziehung der Chipkarte in Datenverarbeitungssysteme entsteht andererseits wieder ein zusätzliches Sicherheitsrisiko, weil Chipkarten relativ leicht verlorengehen können. Es muß deshalb unbedingt dafür gesorgt werden, daß die Chipkarte bei Verlust in jedem Fall vor einem eventuellen Mißbrauch geschützt ist. Die Chipkarte ist deshalb so konzipiert, daß auf die in einer gesicherten Chipkarte gespeicherten Daten nur dann zugegriffen werden kann, wenn vom Benutzer vorab ein nur in der Chipkarte abgespeicherter Identifikator, beispielsweise eine persönliche Identifikationsnummer, die sogenannte PIN, eingegeben wird.

Eine weitere Sicherheitsbarriere kann mit Hilfe der Authentifikation der Chipkarte zum System aufgebaut werden. Diese Authentifikation verhindert, daß ein beliebiger Teilnehmer durch die Vorgabe befugt zu sein, an geheime Informationen im System gelangen kann. Eine wesentliche Voraussetzung für die Authentifikation ist ein persönliches, nicht kopierbares Merkmal des Teilnehmers. Dieses nichtkopierbare Merkmal des Teilnehmers wird mit Hilfe eines geheimen Schlüssels für die Ver-und Entschlüsselung erreicht, der den beiden Partnern, das heißt einerseits der Chipkarte und andererseits dem System, und zwar nur diesen beiden Partnern bekannt ist. Die Sicherheit kann zusätzlich noch dadurch erhöht werden, daß in der Chipkarte unter Einbeziehung dieses geheimen Schlüssels eine Zufallszahl generiert wird, die von der Chipkarte an das System übertragen wird. Es wäre an sich denkbar, dieses Zufallszahlen programmtechnisch zu erzeugen. Nach Ansicht von Sicherheitsexperten sind derart erzeugte Zufallszahlen aber nicht zufällig genug und damit letztlich nicht sicher genug.

Der vorliegenden Erfindung liegt nun die Aufgabe zugrunde, für die Erzeugung von Zufallszahlen einen höchsten Sicherheitsanforderungen genügenden Realisierungsweg aufzuzeigen.

Die Lösung dieser Aufgabe ergibt sich erfindungsgemnäß durch die kennzeichnenden Merkmale des Anspruchs 1. Die Einbeziehung eines variablen Startwertes bei der Generierung der Zufallszahl ermöglicht eine dynamische Authentifizierung mit dem Vorteil, daß die jeweils generierte Zufallszahl im Hinblick auf die geforderten Sicherheitskritierien auch genügend zufällig ist.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben. So sind bezüglich des variablen Startwertes für den Zufallszahlengenerator je nach Art der Chip karte verschiedene Möglichkeiten denkbar. Für den Fall, daß im integrierten Baustein der Chipkarte ein batteriebetriebener Echtzeit-Uhrenbaustein implementiert ist, kann der Startwert aus der jeweils aktuellen Uhrzeit, gegebenenfalls kombiniert mit dem Datum, abgeleitet werden. Eine zweite Möglichkeit besteht darin, daß der Speicherbereich des Chips variable Daten enthält und daß der Startwert aus ausgewählten Daten dieses Speicherbereichs gewonnen wird. Schließlich kann der Startwert auch von außen über ein Terminal an die Chipkarte übergeben werden.

Eine weitere vorteilhafte Ausgestaltung der Erfindung ergibt sich durch eine Einrichtung zur Speicherung der Zufallszahl und durch eine logische Verknüpfung einer variablen Eingangsgröße mit der gespeicherten Zufallszahl zu einem modifizierten variablen Startwert. Dies hat den Vorteil, daß durch die Modifizierung eines variablen Starwertes mit einer bereits vorher generierten Zufallszahl eine neue, beliebig, "zufällige" Zufallszahl generierbar ist.

Im folgenden werden Ausführungsbeispiele der Erfindung anhand der Zeichnung näher erläutert.

Dabei zeigen

FIG 1, 2 je eine Chipkarte mit einem durch einen variablen Startwert angestoßenen Zufallsgenerator

FIG 3, 4 ein Beispiel für einen Zufallszahlengenerator in der Start-und in der Signalausgabephase.

FIG 5 eine Weiterbildung der Schaltungsanodnungen gemäß FIG 1 oder 2.

Die FIG 1 zeigt den prinzipiellen Aufbau einer Prozessor-Chipkarte, die einen im integrierten Baustein implementierten Zufallsgenerator enthält. Die Generierung der Zufallszahlen erfolgt mit Hilfe des gespeicherten Geheimschlüssels K und eines im Mikroprozessor implementierten Chiffrieralgorithmus f, wobei zur Berechnung einer ausreichend "zufälligen" Zufallszahl v ein variabler Startwert s als Eingangsgröße für den Zufallsgenerator verwendet wird. Dieser variable Startwert s kann, wie aus FIG 1 ersichtlich, aus dem Ausgangssignal eines im integrierten Baustein implementierten Echtzeit-Uhrenbausteins T gewonnen werden. Diese Maßnahme setzt allerdings voraus, daß die Chipkarte eine Batterie zur Speisung des Uhrenbausteins T enthält.

Eine etwas einfachere Lösung sieht das Ausführungsbeispiel nach FIG 2 vor, bei dem der Startwert für den Zufallszahlengenerator aus im Chip gespeicherten variablen Daten VD abgeleitet bzw. ausgewählt wird. Schließlich besteht auch noch die Möglichkeit, den Startwert nicht in der Chipkarte selbst zu generieren, sondern diesen Startwert von außen an die Chipkarte zu übergeben.

Die Figuren 3 und 4 zeigen einen in der Chipkarte nach den Figuren 1 und 2 verwendbaren Zufallszahlengenerator, der zum Beispiel auf einem nichtlinear rückgekoppelten Schieberegister basiert. Im einzelnen besteht dieser Zufallszahlengenerator aus einem Schieberegister SR von der Länge r, dem am Eingang der Startwert s mit zum Beispiel 64 Bit zugeführt wird. Durch eine Linearkombination einzelner Registerzellen wird der Inhalt dieser Zellen mit dem Ausgang des Schieberegisters verknüpft. Der zyklusweise durchgeschobene Inhalt des Schieberegisters SR wird in einem nachfolgenden Baustein R einer vom Schlüssel K (zum Beispiel 64 Bit) abhängigen nichtlinearen Funktion unterworfen. Der Ausgang dieses Bausteins R wird während der Zyklusphase auf den Eingang des Schieberegisters SR zurückgekoppelt. FIG 4 zeigt den Zeitpunkt nach Abschluß der Zyklusphase, bei dem die Zufallszahl v mit ebenfalls 64 Bit am Ausgang des Bausteins R zur Verfügung steht.

Die FIG 5 zeigt eine Weiterbildung der Anordnungen nach FIG 1 oder 2 insofern, als der Startwert s nicht unmittelbar aus dem Ausgangssignal des Uhrenbausteins T oder aus variablen Daten VD (erste Eingangsgröße E) gebildet wird, sondern daß zusätzlich eine logische Verknüpfung mit einer weiteren Eingangsgröße stattfindet. Diese weitere Eingangsgröße ist eine vorher erzeugte Zufallszahl v, die in einem Register, beispielsweise in einem Register eines elektrisch löschbaren programmierbaren Lesespeichers EEPROM oder in einem Schreib-Lesespeicher RAM zwischengespeichert ist. Durch die logische Verknüpfung, beispielsweise mit Hilfe eines EXKLUSIV-ODER-Gliedes, werden selbst bei gleichgebliebener erster Eingangsgröße E ein geänderter Startwert s' und eine entsprechend geänderte neue Zufallszahl v generiert. Da für die allererste Generierung einer Zufallszahl v noch keine "alte" Zufallszahl zur Verfügung steht, wird vorgeschlagen, bei der Personalisierung des Sicherheitsmoduls bzw. der Chipkarte einen zufallsgenerierten "Ur-Startwert" US in das Register R einzuschreiben.

Ansprüche

1. Schaltungsanordnung zur Sicherung des Zugriffs zu einem Datenverarbeitungssystem mit Hilfe einer Chipkarte, deren integrierter Baustein einen Mikroprozessor enthält, unter Verwendung eines gemeinsamen, sowohl in der Chipkarte als auch in einem zugehörigen Benutzerterminal hinterlegten Geheimschlüssels, **dadurch gekennzeichnet,** daß im Mikroprozessor ein Chiffrieralgorithmus (f) implementiert ist und daß aus dem Chiffrieralgorithmus (f) und dem Geheimschlüssel (K) in Abhängigkeit von einem variablen Startwert (s) eine Zufallszahl (v) gemäß der Beziehung

$$v = f(K;s)$$

generierbar ist.

2. Schaltungsanordnung nach Anspruch 1, **dadurch gekennzeichnet,** daß der Startwert (s) aus im integrierten Baustein der Chipkarte gespeicherten Daten ausgewählt wird.

3. Schaltungsanordnung nach Anspruch 1, **dadurch gekennzeichnet,** daß der Startwert (s) durch das Ausgangssignal einer im Chip integrierten Echtzeit-Uhrenschaltung (T) gebildet ist.

4. Schaltungsanordnung nach Anspruch 1, **dadurch gekennzeichnet,** daß der Startwert (s) von außen zuführbar ist.

5. Schaltungsanordnung nach einem der vorhergehenden Ansprüche, **gekennzeichnet** durch eine Einrichtung zur Speicherung der Zufallszahl (v) und durch eine logische Verknüpfung einer variablen Eingangsgröße (E) mit der gespeicherten Zufallszahl (v) zu einem modifizierten Startwert (s').

6. Schaltungsanordnung nach Anspruch 5, **dadurch gekennzeichnet,** daß als erster Speichereintrag ein das Sicherheitsmodul personalisierenden Ur-Startwert (US) einspeicherbar ist.

7. Schaltungsanordnung nach einem der vorhergehenden Ansprüche, **gekennzeichnet** durch ein Schieberegister (SR) mit einer Linearkombination einzelner Registerzellen, dem eingangsseitig

der Startwert (s) zuführbar ist und durch einen mit dem Ausgang des Schieberegisters verbundenen nichtlinearen Funktionsbaustein, dessen vom Geheimschlüssel (K) abhängiges Ausgangssignal während einer Zyklusphase an den Eingang des Schieberegisters (SR) zurückgekoppelt ist.

8. Schaltungsanordnung nach Anspruch 7, **dadurch gekennzeichnet,** daß nach Abschluß der Zyklusphase am Ausgang des Funktionsbausteins die jeweils generierte Zufallszahl (v) erscheint.

FIG 1

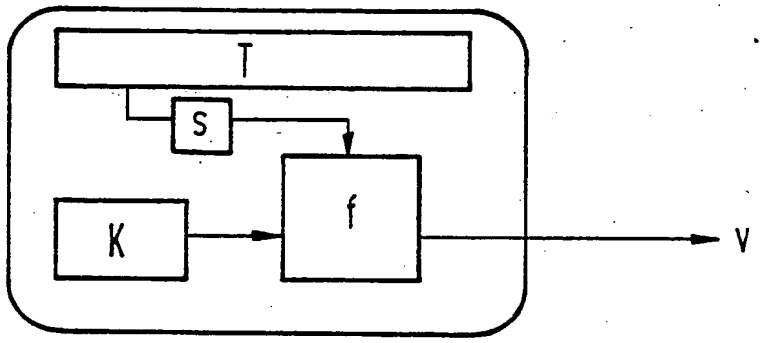


FIG 2

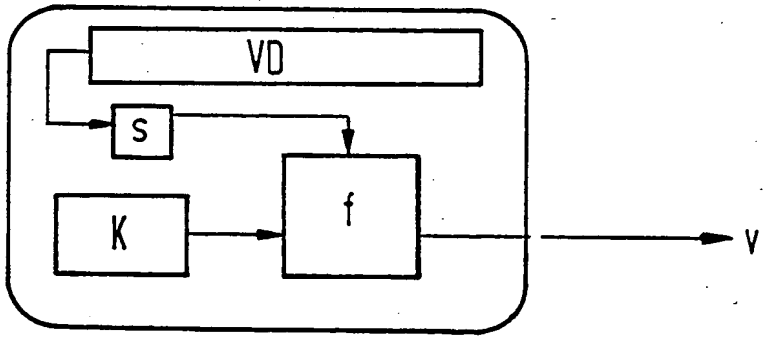


FIG 3

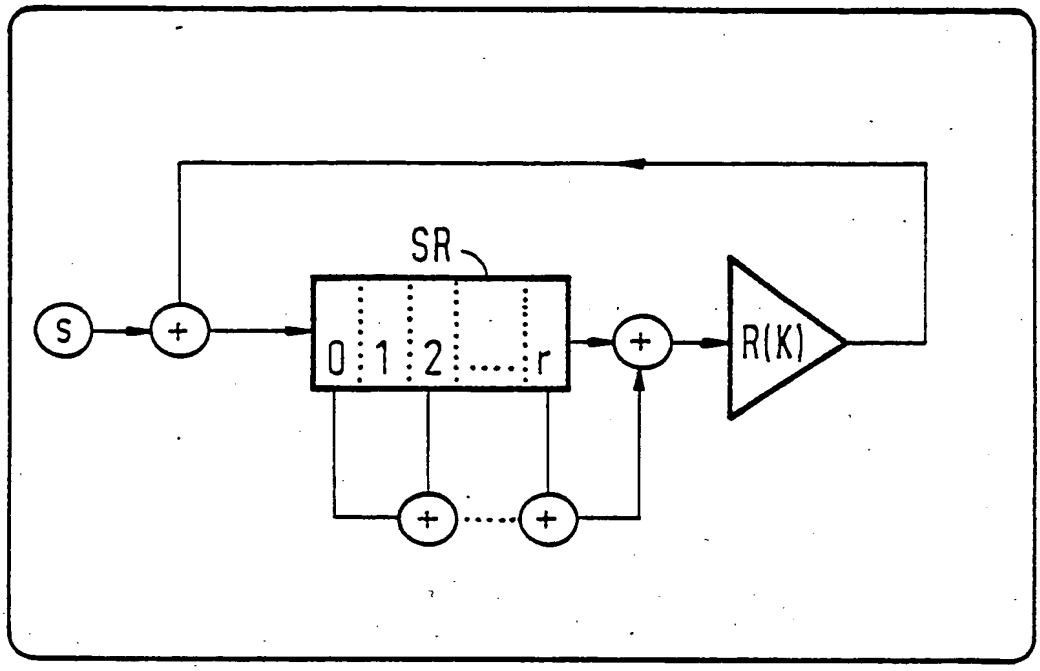


FIG 4

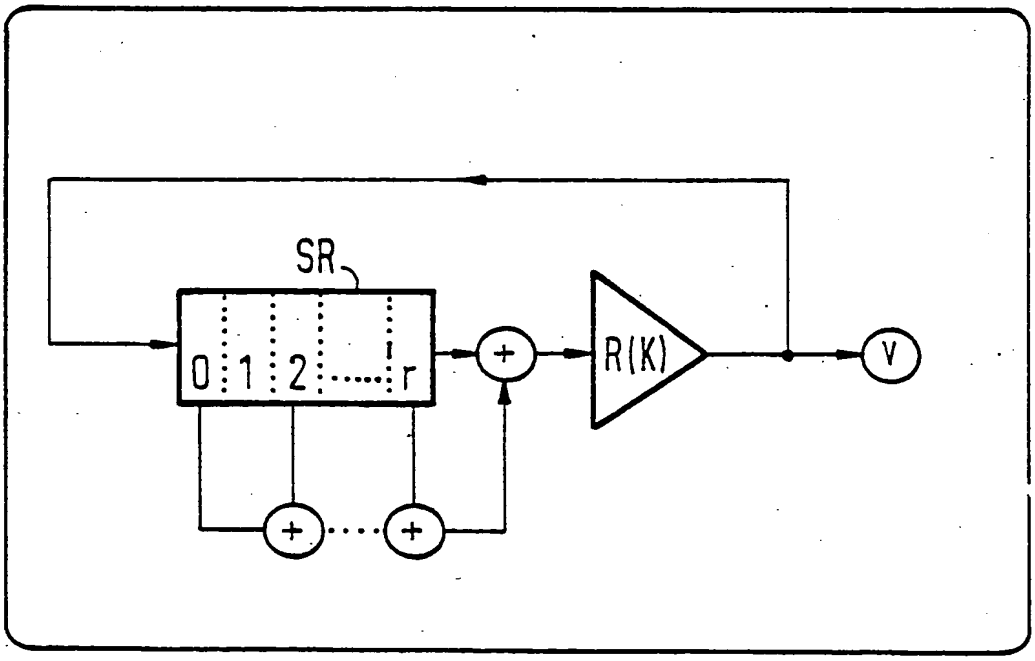
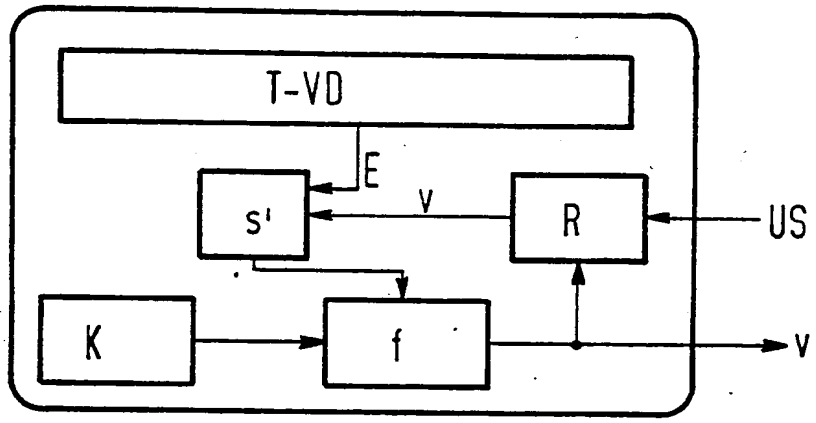


FIG 5



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 281 057**
A3

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 88103012.6

(51) Int. Cl.[5] G07F 7/10 , G07C 9/00

(22) Anmeldetag: 29.02.88

(30) Priorität: 04.03.87 DE 3706955
12.08.87 DE 3726881

(43) Veröffentlichungstag der Anmeldung:
07.09.88 Patentblatt 88/36

(84) Benannte Vertragsstaaten:
AT BE CH DE ES FR GB IT LI LU NL SE

(88) Veröffentlichungstag des später veröffentlichten Recherchenberichts: 18.04.90 Patentblatt 90/16

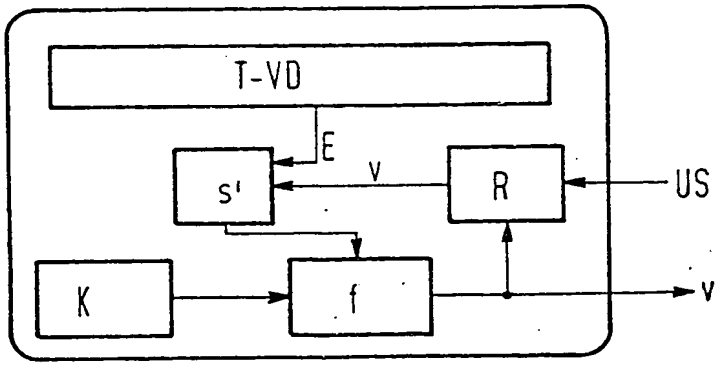
(71) Anmelder: **Siemens Aktiengesellschaft**
Wittelsbacherplatz 2
D-8000 München 2(DE)

(72) Erfinder: **Beutelspacher, Albrecht, Prof.**
Schwalbenstrasse 78
D-8012 Ottobrunn(DE)
Erfinder: **Kersten, Annette-Gabriele**
Frauenlobstrasse 6
D-6200 Wiesbaden(DE)
Erfinder: **Kruse, Dietrich**
Ulmenstrasse 9
D-8012 Ottobrunn(DE)

(54) Schaltungsanordnung zur Sicherung des Zugangs zu einem Datenverarbeitungssystem mit Hilfe einer Chipkarte.

(57) Aus einem im Mikroprozessor der Chipkarte implementierten Chiffrieralgorithmus (f) und einem gespeicherten Geheimschlüssel (K) wird in Abhängigkeit von einem variablen Startwert (s) eine Zufallszahl gemäß der Beziehung v = f(K; s) generiert. Diese Zufallszahl kann in einem Register zwischengespeichert und bei der Generierung einer neuen Zufallszahl mit einer variablen Eingangsgröße, z.B. mit dem variablen Startwert (s) zu einem modifizierten variablen Startwert (s') logisch verknüpft werden.

FIG 5



EP 0 281 057 A3

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 88 10 3012

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.4)
A	EP-A-0140013 (IBM DEUTSCHLAND) * Zusammenfassung; Ansprüche 1, 2 * * Seite 5, Zeile 3 - Seite 6, Zeile 20 * * Seite 7, Zeile 7 - Seite 10, Zeile 23 * ---	1-8	G07F7/10 G07C9/00
A	EP-A-0148960 (I.B.M.-INTERNATIONAL BUSINESS MACHINES CORPORATION) * Zusammenfassung; Ansprüche 1-4 * * Seite 5, Zeile 1 - Seite 14, Zeile 20 * ---	1, 3, 5-7	
A	EP-A-0055986 (TRANSAC-ALCATEL-COMP. POUR LE DEVELOPM. DES TRANSACT. AUTOMAT.) * Zusammenfassung; Ansprüche 1-8 * ---	1, 2, 4-6	
A	EP-A-0063794 (SIEMENS AKTIENGESELLSCHAFT) * Zusammenfassung; Ansprüche 1-8; Figuren 1-6 * ---	1-3	
A	EP-A-0138320 (VISA U.S.A. INC.) * Zusammenfassung; Ansprüche 1, 3-7, 12-15; Figuren 1-6 * -----	1	

RECHERCHIERTE SACHGEBIETE (Int. Cl.4)
G07F G07C H04L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	19 FEBRUAR 1990	GUIVOL O.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P0403)